

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-39483

(43) 公開日 平成11年(1999) 2月12日

(51) Int.Cl.⁸

G 0 6 T 7/00

G 0 6 K 17/00

識別記号

F I

G 0 6 F 15/62

G 0 6 K 17/00

4 6 0

V

審査請求 未請求 請求項の数16 O L (全 14 頁)

(21) 出願番号

特願平9-191335

(22) 出願日

平成9年(1997) 7月16日

(71) 出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 重松 智志

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74) 代理人 弁理士 伊東 忠彦

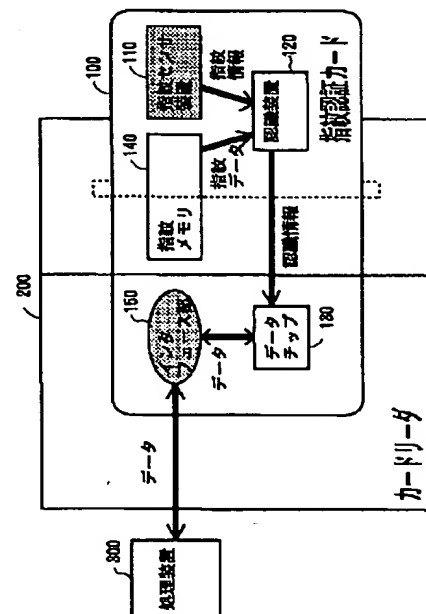
(54) 【発明の名称】 指紋認証カード、メモリカード、認証システム、認証装置及び携帯機器

(57) 【要約】

【課題】 ユーザやサービス装置の作業を簡略化すると共に、暗証番号やパスワードの盗難等による被害からユーザ及びサービス提供者を守ることが可能な指紋認証カード及び認証システムを提供する。

【解決手段】 本発明は、指紋による凹凸を検知するセンサ回路からなり、接触した指の指紋情報を検出するセンサ手段と、種々の情報を記録するデータ記録手段とを有する指紋認証カードと、指紋認証カードを読み取るカードリーダー200とを有する。指紋認証カードは、センサ手段で検出した指紋情報と、指紋記憶手段に登録されている指紋データとの照合を行い、照合結果を出力する認識手段とを有する。また、カードリーダーに接続されたサービス装置を更に有し、カードリーダーは、ユーザの照合結果が有効な場合に、ユーザ記録手段に格納されているユーザ情報をサービス装置に送信する手段を含む。

本発明の認証システムの構成図



【特許請求の範囲】

【請求項1】 データ記憶手段と、

指紋による凹凸を検知するセンサ回路からなり接触した指の指紋情報を検出するセンサ手段とを有することを特徴とする指紋認証カード。

【請求項2】 指紋データを予め登録しておく指紋記憶手段と、

前記センサ手段で検出した指紋情報と、前記指紋記憶手段内の指紋データとの照合を行い、照合結果を送信する認識手段と、

前記認識手段からの照合結果に基づいて前記データ記憶手段の読出し、または、書込みを可能とするデータチップとを更に有する請求項1記載の指紋認証カード。

【請求項3】 前記データ記憶手段を読出し専用とする請求項2記載の指紋認証カード。

【請求項4】 指紋による凹凸を検知するセンサを有し、接触した指の指紋情報を検出するセンサ手段と、指紋データを予め登録しておく指紋記憶手段と、前記センサ手段で検出した指紋情報と、前記指紋記憶手段内の指紋データとの照合を行い、照合結果を送信する認識手段と、前記照合結果を取得し、該照合結果に基づいてメモリカード内のメモリへの読出し、または、書込みを可能とするメモリデータ送信手段とを有することを特徴とするメモリカード。

【請求項5】 データ記憶手段と、指紋により凹凸を検知するセンサ回路からなり、接触した指の指紋情報を検出するセンサ手段と、指紋データを予め登録しておく指紋記憶手段と、前記センサ手段で検出した指紋情報と、前記指紋記憶手段内の指紋データとの照合を行い、照合結果を送信する認識手段と、前記認識手段からの照合結果に基づいて前記データ記憶手段の読出し、または、書込みを可能とするデータチップとを有する指紋認証カードと、さらに、前記指紋認証カードを読み取るカードリーダーとを有し、前記指紋認証カードが前記カードリーダーに挿入され、前記指紋認証カード中の前記センサ手段に指を接触させたとき、該センサ手段は、検出した指紋情報と前記指紋記憶手段内の指紋データとを前記認識手段で照合し、前記データチップは、該指紋情報が該指紋データと同一という照合結果を取得した場合に、前記カードリーダーとの間で前記データ記憶手段の読出し、または、書込みを可能とすることを特徴とする認証システム。

【請求項6】 前記カードリーダーに接続されるサービス装置を更に有し、前記指紋認証カードは、前記認識手段での照合が有効である場合に、前記データ記憶手段中のデータを前記サービス装置に送信し、

前記サービス装置は、所定のサービスを行う請求項5記載の認証システム。

【請求項7】 前記カードリーダーに接続された検索手段と、

前記検索手段に接続されたデータベースと、

サービス装置とを更に有し、

照合が有効である時に、前記データ記憶手段中のデータをさらに、前記検索手段に送信し、前記検索手段が該データを用いて前記データベースを検索して得た情報に基づいて、前記サービス装置が所定のサービスを行う請求項5記載の認証システム。

【請求項8】 データ記憶手段と、

指紋による凹凸を検知するセンサ回路からなり、接触した指の指紋情報を検出するセンサ手段とを有する指紋認証カードと、

カードリーダーとを有し、

前記指紋認証カードが前記カードリーダーに挿入され、前記センサ手段に指を接触させた時、前記指紋認証カード中の前記センサ手段で検出した指紋情報及び前記データ記憶手段に記憶されたデータを前記カードリーダーに送信することを特徴とする認証システム。

【請求項9】 前記カードリーダーに接続された認証手段と、

前記認証手段に接続された指紋が登録された指紋データベースと、

サービス装置とをさらに有し、

前記指紋情報及び前記データ記憶手段に記憶されたデータをさらに、前記認証装置に送信し、

前記認証装置は、前記指紋データベースにアクセスして、前記データ記憶手段に記憶されたデータから登録された指紋データを検索し、前記指紋情報との照合を行い、照合が有効であるとき、前記サービス装置が所定のサービスを行う請求項8記載の認証システム。

【請求項10】 前記カードリーダーに接続される蓄積手段と、

前記蓄積手段に接続された利用履歴データベースとを更に有し、

前記指紋情報及び前記データ記憶手段に記憶されたデータを、前記蓄積手段に送信し、

前記蓄積装置は、前記利用履歴データベースにアクセスして、前記指紋情報及び前記データ記憶手段に記憶されたデータを書き込む請求項8記載の認証システム。

【請求項11】 暗号化手段及び暗号復号手段とを更に有し、

前記カードリーダーと前記認証手段または、前記蓄積手段との間で、前記指紋情報及び、前記データ記憶手段に記憶されたデータを暗号化して伝送する請求項9または、10記載の認証システム。

【請求項12】 前記データ記憶手段内のデータは、前記指紋認証カードのユーザに関する情報である請求項

10

20

30

40

50

6、9、10または、11記載の認証システム。

【請求項13】 データ記憶手段内のデータは、前記指紋認証カードのユーザの識別コードである請求項7、

9、10または、11記載の認証システム。

【請求項14】 指紋による凹凸を検知するセンサ回路からなり、接触した指の指紋情報を検出するセンサ手段と、

指紋データを予め登録しておく指紋記憶手段と、

前記センサ装置で検出した指紋情報と、前記指紋記憶手段内の指紋データとの照合を行い、照合結果を送信する認識手段と、

メモリと、

前記照合結果を取得し、該照合結果に基づいて前記メモリへ読出し、または、書込みを可能とするメモリデータ送受信手段とを有するメモリカードと、

カードを挿入するスロットと、

処理装置とを具備し、

前記メモリカードが、前記スロットに挿入され、該メモリカード中の前記センサ手段に指を接触させたとき、前記指紋記憶手段中の指紋データと前記センサ手段で検出した指紋情報とを前記認証装置で照合し、

前記照合が有効である時に、前記メモリカード中の前記メモリと前記処理装置との間でメモリデータ送受信装置を介してデータの送受を可能とすることを特徴とする認証システム。

【請求項15】 指紋による凹凸を検出するセンサ回路を有し、接触した指の指紋情報を検出するセンサ手段と、

指紋データを予め登録しておく、指紋記憶手段と、

前記センサ手段で検出した指紋情報と、前記指紋記憶手段内の指紋データとの照合を行い、照合結果を送信する認識手段と、

前記照合結果を取得して動作する電源回路とを具備し、前記センサ手段に指を接触させたとき、前記指紋記憶手段内の指紋データと、前記センサ手段で検出した指紋情報とを前記認識手段で照合し、前記照合結果が有効である場合のみ前記電源回路が動作することを特徴する認証装置。

【請求項16】 指紋による凹凸を検出するセンサ回路を有し、接触した指の指紋情報を検出するセンサ手段と、

指紋データを予め登録しておく、指紋記憶手段と、

前記センサ手段で検出した指紋情報と、前記指紋記憶手段内の指紋データとの照合を行い、照合結果を送信する認識手段と、

前記照合結果を取得して動作する電源回路と、

前記センサ手段に指を接触させたとき、前記指紋記憶手段内の指紋データと、前記センサ手段で検出した指紋情報とを前記認識手段で照合し、前記照合結果が有効である場合のみ前記電源回路が動作する認証装置とを具備

し、

前記認証装置における前記電源回路を電源として用いることを特徴とする携帯機器。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、指紋認証カード、メモリカード、認証システム及び認証装置及び携帯機器に係り、特に、あるサービスを受けようとするユーザに、そのユーザ本人である場合のみにサービスを提供する装置に対し、ユーザが指紋認識装置を埋め込んだカードを用いて暗証番号やパスワード等で行っているユーザの認証を指紋情報を用いて行うための指紋認証カード、メモリカード、認証システム及び認証装置及び携帯機器に関する。

【0002】

【従来の技術】図14は、従来の第1の認証システムを説明するための図である。従来の第1の方法では、ユーザがサービスを利用する時、まず、ユーザのカード12をカードリーダー10に挿入する。次に、ユーザはカード作成時に決めた暗証を暗証入力装置を用いて入力する。認証装置15がこの入力された暗証情報とカード12に記録された暗証データとを用いて照合を行い、その結果をサービス装置16に送信する。サービス装置16は、認証結果が有効であった時のみサービスを提供する。

【0003】図15は、従来の第2の認証システムを説明するための図である。同図に示す手法は、図14の暗証入力装置14の代わりに、指紋読み取り装置17を用い、ユーザは暗証の入力の代わりに指紋読み取り装置の上に指を乗せて指紋を入力する。認証装置15は、予め登録されている指紋データベース18からカードに登録されているユーザ識別コードに対応する指紋データを読み込み、指紋読み取り装置17が送信した指紋情報との照合を行い、その結果をサービス装置16に送信する。サービス装置16は、認証結果が有効であった時のみサービスを提供する。

【0004】

【発明が解決しようとする課題】しかしながら、上記従来の第1の方法では、正しい暗証を知っていれば、ユーザは本人でなくともサービスの提供を受けることができる。これでは、暗証の盗難時の不正利用等の被害を防ぐことはできないという問題がある。また、上記従来の第2の方法では、暗証の盗難時の事故を防ぐことは可能であるが、各ユーザの指紋データを予め各サービス装置16の指紋データベース18に登録しておく必要がある。また、このデータベースを共有化した場合、認証時のデータ通信に時間が必要となり認識に多くの時間がかかってしまう。

【0005】さらに、このデータベース18のデータが盗難された場合、非常に多くの個人情報流出してしまう恐れがある。また、指紋読み取り装置17が認証装置

15と物理的に分離しているため指紋データ送信時にこのデータに不正な細工をされてしまうと、正確な認証が行えないという問題がある。本発明は、上記の点に鑑みなされたもので、ユーザやサービス装置の作業を簡略化すると共に、暗証番号やパスワードの盗難等による被害からユーザ及びサービス提供者を守ることが可能な指紋認証カード、メモリカード、認証システム及び認証装置及び携帯機器を提供することを目的とする。

【0006】

【課題を解決するための手段】本発明の指紋認証カードは、データ記憶手段と、指紋による凹凸を検知するセンサ回路からなり接触した指の指紋情報を検出するセンサ手段とを有する。また、本発明の指紋認証カードは、指紋データを予め登録しておく指紋記憶手段と、センサ手段で検出した指紋情報と、指紋記憶手段内の指紋データとの照合を行い、照合結果を送信する認識手段と、認識手段からの照合結果に基づいてデータ記憶手段の読出し、または、書込みを可能とするデータチップとを更に有する。

【0007】また、本発明の指紋認証カードは、データ記憶手段を読出し専用とする。また、本発明のメモリカードは、指紋による凹凸を検知するセンサを有し、接触した指の指紋情報を検出するセンサ手段と、指紋データを予め登録しておく指紋記憶手段と、センサ手段で検出した指紋情報と、指紋記憶手段内の指紋データとの照合を行い、照合結果を送信する認識手段と、照合結果を取得し、該照合結果に基づいてメモリカード内のメモリへの読出し、または、書込みを可能とするメモリデータ送信手段とを有する。

【0008】本発明の認証システムは、データ記憶手段と、指紋により凹凸を検知するセンサ回路からなり、接触した指の指紋情報を検出するセンサ手段と、指紋データを予め登録しておく指紋記憶手段と、センサ手段で検出した指紋情報と、指紋記憶手段内の指紋データとの照合を行い、照合結果を送信する認識手段と、認識手段からの照合結果に基づいてデータ記憶手段の読出し、または、書込みを可能とするデータチップとを有する指紋認証カードと、さらに、指紋認証カードを読み取るカードリーダを有し、指紋認証カードがカードリーダに挿入され、指紋認証カード中のセンサ手段に指を接触させたとき、該センサ手段は、検出した指紋情報と指紋記憶手段内の指紋データとを認識手段で照合し、データチップは、該指紋情報が該指紋データと同一という照合結果を取得した場合に、カードリーダとの間でデータ記憶手段の読出し、または、書込みを可能とする。

【0009】また、本発明の認証システムは、カードリーダに接続されるサービス装置を更に有し、指紋認証カードは、認識手段での照合が有効である場合に、データ記憶手段中のデータをサービス装置に送信し、サービス装置は、所定のサービスを行う。

【0010】また、本発明の認証システムは、カードリーダに接続された検索手段と、検索手段に接続されたデータベースと、サービス装置とを更に有し、照合が有効である時に、データ記憶手段中のデータを、さらに、検索手段に送信し、検索手段が該データを用いてデータベースを検索して得た情報に基づいて、サービス装置が所定のサービスを行う。

【0011】また、本発明の認証システムは、データ記憶手段と、指紋による凹凸を検知するセンサ回路からなり、接触した指の指紋情報を検出するセンサ手段とを有する指紋認証カードと、カードリーダとを有し、指紋認証カードがカードリーダに挿入され、センサ手段に指を接触させた時、指紋認証カード中のセンサ手段で検出した指紋情報及びデータ記憶手段に記憶されたデータをカードリーダに送信する。

【0012】また、本発明の認証システムは、カードリーダに接続された認証手段と、認証手段に接続された指紋が登録された指紋データベースと、サービス装置とを更に有し、指紋情報及びデータ記憶手段に記憶されたデータをさらに、認証装置に送信し、認証装置は、指紋データベースにアクセスして、データ記憶手段に記憶されたデータから登録された指紋データを検索し、指紋情報との照合を行い、照合が有効であるとき、サービス装置が所定のサービスを行う。

【0013】また、本発明の認証システムは、カードリーダに接続される蓄積手段と、蓄積手段に接続された利用履歴データベースとを更に有し、指紋情報及びデータ記憶手段に記憶されたデータを蓄積手段に送信し、蓄積装置は、利用履歴データベースにアクセスして、指紋情報及びデータ記憶手段に記憶されたデータを書き込む。

【0014】また、本発明の認証システムは、暗号化手段及び暗号復号手段とを更に有し、カードリーダと認証手段または、蓄積手段との間で、指紋情報及び、データ記憶手段に記憶されたデータを暗号化して伝送する。また、本発明の認証システムは、データ記憶手段内のデータは、指紋認証カードのユーザに関する情報である。

【0015】また、本発明の認証システムは、データ記憶手段内のデータは、指紋認証カードのユーザの識別コードである。また、本発明の認証システムは、指紋による凹凸を検知するセンサ回路からなり、接触した指の指紋情報を検出するセンサ手段と、指紋データを予め登録しておく指紋記憶手段と、センサ装置で検出した指紋情報と、指紋記憶手段内の指紋データとの照合を行い、照合結果を送信する認識手段と、メモリと、照合結果を取得し、該照合結果に基づいてメモリへ読出し、または、書込みを可能とするメモリデータ送受信手段とを有するメモリカードと、カードを挿入するスロットと、処理装置とを具備し、メモリカードが、スロットに挿入され、該メモリカード中のセンサ手段に指を接触させたとき、指紋記憶手段中の指紋データとセンサ手段で検出した指

紋情報とを認証装置で照合し、照合が有効である時に、メモリカード中のメモリと処理装置との間でメモリデータ送受信装置を介してデータの送受を可能とする。

【0016】また、本発明の認証装置は、指紋による凹凸を検出するセンサ回路を有し、接触した指の指紋情報を検出するセンサ手段と、指紋データを予め登録しておく、指紋記憶手段と、センサ手段で検出した指紋情報と、指紋記憶手段内の指紋データとの照合を行い、照合結果を送信する認識手段と、照合結果を取得して動作する電源回路とを具備し、センサ手段に指を接触させたとき、指紋記憶手段内の指紋データと、センサ手段で検出した指紋情報とを認識手段で照合し、照合結果が有効である場合のみ電源回路が動作する。

【0017】本発明の携帯機器は、指紋による凹凸を検出するセンサ回路を有し、接触した指の指紋情報を検出するセンサ手段と、指紋データを予め登録しておく、指紋記憶手段と、センサ手段で検出した指紋情報と、指紋記憶手段内の指紋データとの照合を行い、照合結果を送信する認識手段と、照合結果を取得して動作する電源回路とを有し、センサ手段に指を接触させたとき、指紋記憶手段内の指紋データと、センサ手段で検出した指紋情報とを認識手段で照合し、照合結果が有効である場合のみ電源回路が動作する認証装置とを具備し、認証装置における電源回路を電源として用いることを可能とする。

【0018】上記のように、本発明では、予め登録しておいた指紋と入力した指紋とを照合し、本人であることを確認する指紋認識装置を組み込んだカードを利用して、そのカードを持っているユーザの認証を行う。カードリーダーが接続され、カードを用いて処理を行う処理装置は、指紋認証装置の認証機能を有する部分にカードの持主が指を当てている場合のみカードの中身（カードデータ部分等）にアクセスが可能になる。つまり、カードを使っている人がこのカードの持主である場合のみこのカードは有効になる。

【0019】これにより、盗難される恐れのある暗証が不要となり、例えば、カードが盗難された場合でもカード内の認証装置が認証を確認しない限りカードのデータにアクセスできないため、不正に利用される恐れがない。また、ユーザの指紋情報は、それぞれのカードに格納されるため集中管理の必要がなく、高速に認証を行うことが可能であり、個人情報の流出の心配もない。

【0020】さらに、指紋認証装置と指紋読み取り装置は、同一チップ内に形成されるため、これらの装置間に細工を行い、不正に認識データを改ざんすることは殆ど不可能である。また、指紋データとして複数の人のデータを記録しておくことで、家族カード等のグループカードも実現可能である。

【0021】また、マネーカードやクレジットカードに応用可能であり、カード利用時に認証が確認されたときのみカード間のデータにアクセスが可能となり電子マネ

ー等のやりとりが可能となる。

【0022】

【発明の実施の形態】図1は、本発明の認証システムの構成を示す。同図に示す認証システムは、指紋認証カード100、カードリーダー200、及び処理装置300から構成される。指紋認証カード100は、指紋センサ装置110、認識装置120、データチップ130、指紋メモリ140、インタフェース部150から構成される。

10 【0023】なお、指紋認証カード100の指紋センサ装置110は、指紋による凹凸を電気信号に変換するセンサ回路を複数敷きつめ、指を接触されることにより、指紋を読み取るものである。また、指紋メモリ140は、メモリ回路から構成されている。指紋センサ装置110は、大きさ数 μm のセンサ回路を並べたものである。図2は、本発明の指紋認証カードに搭載される指紋センサ装置を説明するための図である。同図に示すように、センサ回路は、例えば、指の接触面の静電容量を測定し、接触面が触れている部分の指紋の凹凸を検出す

20 【0024】認証装置120は、指紋センサ装置110で検出した指紋情報と、指紋メモリ140内の指紋データとの照合を行い、照合結果を送付する。データチップ130は、その内部にメモリなどの記憶手段を有する。指紋メモリ140は、指紋データを予め登録しておく。ユーザが指紋認証カード100をカードリーダー200に挿入し、認識装置120の上に指を載せる。認識装置120は、読み取った指紋と指紋メモリ140に記録されている指紋との照合を行い、その照合結果（認識結果）をデータチップ130に転送する。

30 【0025】データチップ130は、認識結果が有効であるという信号を受けた場合、その内部の記憶手段に保持されているユーザ情報などの情報をカードリーダー200を介して接続された処理装置300に送付するほか、処理装置300からカードリーダー200を介して当該データを受け取り、内部の記憶手段に記憶する。これによりユーザが指紋認証カード100の正当な所有者であるときのみ処理装置300は、指紋認証カード100内に記録されたデータを用いて所定の処理を行う。

40 【0026】

【実施例】以下、図面と共に本発明の実施例を説明する。

【第1の実施例】本発明の第1の実施例として指紋認証カード100のデータチップ130にユーザ情報を記録した読出し専用メモリを用いた例を説明する。

【0027】図2は、本発明の第1の実施例の認証システムの構成を示す。同図において図1と同一構成部分には同一符号を付与し、その説明を省略する。同図に示す認証システムは、図1に示す構成における処理装置300に代わってサービス装置350を設け、さらに、デー

タチップ 130 内にユーザ情報を格納するための読出し専用メモリであるユーザ情報格納部 131 を設けた構成である。

【0028】本実施例では、ユーザが指紋認証カード 100 をカードリーダー 200 に挿入し、認識装置 120 の上に指を乗せる。これにより指紋センサ装置 110 は、ユーザの指紋を読み取り、認識装置 120 に転送する。認識装置 120 は、読み取った指紋と指紋認証カード 100 内の指紋メモリ 140 内に記録されたユーザの指紋と指紋センサ装置 110 により読み取られたユーザの指紋との照合を行い、その認識情報（照合結果）をデータチップ 130 に送信する。データチップ 130 は、照合が有効である場合のみ、カードリーダー 200 を介して接続されたサービス装置 350 に、データチップ 130 のユーザ情報格納部 131 に記録されたユーザ名、暗証番号等のユーザ情報を送信する。

【0029】サービス装置 300 は、このデータを用いてサービスをユーザに提供する。この手法では、データチップ 130 内のユーザ情報格納部を読出し専用メモリにすることで、カード作成以降に、カード内のデータを改ざんするとが不可能となり、当該指紋認証カード 100 を他人のカードに不正に変更することが不可能となる。

【0030】この方法は、銀行 100 の ATM カードやカードキー等の応用可能であり、ユーザは煩わしい暗証番号の入力から解放される。

〔第 2 の実施例〕次に、本発明の第 2 の実施例として、指紋認証カード 100 のデータチップにユーザ識別コードを記録した読出し専用メモリを有し、カードリーダー 200 の出力をサービス装置 350 に接続した例を説明する。

【0031】図 4 は、本発明の第 2 の実施例の認証システムの構成を示す。同図に示すシステムは、カードリーダー 200 とサービス装置 350 との間に検索装置 400 を接続し、当該検索装置 400 が検索実行時にデータを検索する対象となる識別コードデータベース 500 を検索装置 400 に接続し、さらにデータチップ 130 内にはユーザ識別情報を格納するための読出し専用メモリであるユーザ識別情報格納部 133 を設けた構成である。

【0032】同図において図 1、図 3 と同一構成部分には同一符号を付し、その説明を省略する。本実施例では、前述の第 1 の実施例と同様に、ユーザは指紋認証カード 100 をカードリーダー 200 に挿入し、認識装置 120 の上に指を乗せる。これにより、指紋センサ装置 110 が当該ユーザの指紋を読み取り、認識装置 120 に転送する。認識装置 120 は、読み取ったユーザの指紋と指紋メモリ 140 に記録されている指紋情報との照合を行い、その結果をデータチップ 130 に転送する。データチップ 130 は、照合が有効である場合にのみ、カードリーダー 200 を介して接続された検索装置 400

に、データチップ 130 のユーザ識別情報格納部 133 に記録されたユーザ識別コードを転送する。第 1 の実施例と本実施例の相違点は、以下の通りである。ユーザ情報が大量であった、サービス提供者が管理するサービスの場合など、カード上にユーザ情報を保持することができない場合がある。このときは、本実施例のように、カードからユーザ情報自体を送信するのではなく、ユーザ識別コードを送信し、これを受け取った装置側でデータベースを検索してユーザ情報を得る。

10 【0033】検索装置 400 は、ユーザ情報データベース 500 を検索する。図 5 にユーザ情報データベース 500 に格納されているレコードの例を示す。各ユーザのユーザ識別コードに対応して、氏名、住所、年齢、性別、利用可能サービス等が記録されている。検索の際には、ユーザ識別コードをキーとして、当該指紋認証カード 100 を利用しているユーザを特定し、当該ユーザのユーザ情報をサービス装置 350 に送信する。

20 【0034】サービス装置 350 は、検索装置 400 から送られたデータを用いてサービスをユーザに提供する。この手法では、指紋認証カード 100 をカードリーダー 200 に挿入したユーザが誰であるかを正確に特定することが可能となる。検索装置 400 にユーザ識別コードが転送されるということは、このカードを挿入している人がこのカードの所有者であると認証されていることであり、識別コードデータベース 500 が正確である限り、検索装置 400 が誤認することはない。また、識別コードを複雑なコードにすることで更に安全性を高めることが可能となる。

30 【0035】本実施例の方法によれば、コンピュータのログイン制御など、ユーザを特定する必要があるシステムのユーザ管理を盗難等の恐れのあるパスワードを用いることなく、正確に行うことができる。

〔第 3 の実施例〕本実施例では、前述の実施例のように指紋認証カード 100 上の認識装置 120 を利用せずに、カードリーダー 200 に接続された認証装置を利用する例を説明する。

40 【0036】図 6 は、本発明の第 3 の実施例の認証システムの構成を示す。同図に示す認証システムは、カードリーダー 200 を認証装置 600 に接続し、認証装置 600 の出力をサービス装置 350 に接続したものであり、指紋認証カード 100 には上記の実施例のように認証装置 120 が存在しない構成である。同図に示す指紋認証カード 100 は、指紋センサ装置 110、読出し専用メモリであるユーザ識別コード格納部 133、及びインタフェース部 150 から構成される。

50 【0037】ユーザは、指紋認証カード 100 をカードリーダー 200 に挿入し、指紋センサ装置 110 上に指を乗せる。指紋センサ装置 110 は、指紋を読み取り、当該指紋情報は、ユーザ識別コード格納部 133 に記録されたユーザ識別コードと共に、カードリーダー 200 に接

続された認証装置 600 に転送される。認証装置 600 は、転送された指紋情報とユーザ識別コードとを利用して、指紋データベース 700 に記録されているユーザの指紋との照合を行い、その結果をサービス装置 350 に送信する。指紋データベース 700 に格納されるレコードの例を図 7 に示す。

【0038】サービス装置 350 は、この認証が有効である場合に、サービスをユーザに提供する。なお、本実施例において、指紋認証カード内のユーザ識別コード格納部 133 の代わりに、ユーザ情報を記録した、ユーザ情報格納部 131 を用いてもよい。この場合、ユーザ識別コードの代わりに、ユーザ情報が転送される。

【0039】この手法では、指紋認識を指紋認証カード 100 上の認識装置（実施例 1, 2 (120)）を用いるのではなく、カードリーダー 200 に接続されている認証装置 600 を用いる。ユーザの指紋情報は、指紋認証カード 100 上に保持されずに、外部の指紋データベース 700 に保持されている。これを用いることで、臨時カードや利用回数を制限したカードの実現や、利用可能なサービス装置を制限すること、サービス提供者がユーザの指紋を管理することが可能となる。

【0040】〔第 4 の実施例〕本実施例では、上記の第 3 の実施例におけるカードリーダー 200 からの指紋情報及びユーザ識別コードを暗号化して送信し、受信した側において復号化して指紋情報及びユーザ識別コードを認証する例を説明する。図 8 は、本発明の第 4 の実施例の認証システムの構成を示す。同図において図 6 と同一構成部分については同一符号を付し、その説明を省略する。

【0041】同図に示す認証システムは、上記の第 3 の実施例のカードリーダー 200 に暗号化装置 800 を設け、認証装置 600 の前段に暗号化装置 800 から通信路を介して送信される暗号化情報を復号化する暗号復号装置 900 を設けた構成である。本実施例では、カードリーダー 200 の出力を暗号化装置 800 に入力し、当該暗号化装置 800 において入力された信号（指紋情報及びユーザ識別コード）を暗号化し、通信路を介して暗号復号装置 900 に送信する。暗号復号装置 900 は、受信した暗号化された指紋情報及びユーザ識別コードを復号化して認証装置 600 に出力する。

【0042】ユーザは、指紋認証カード 100 をカードリーダー 200 に挿入し、指紋認証装置 110 の上に指を乗せる。指紋認証装置 110 は、指紋をスキャンし、その結果を暗号化装置 800 に出力する。これにより、暗号化装置 800 は、指紋認証装置 110 から取得した指紋情報及びユーザ識別コードを暗号化して通信路を介して暗号復号装置 900 に送信する。暗号復号装置 900 は、暗号化された指紋情報及びユーザ識別コードを復号して認証装置 600 に出力する。

【0043】認証装置 600 は、復号された指紋情報と

指紋データベース 700 に記録されている指紋情報とを照合して、その認識結果をサービス装置 350 に転送する。これにより、サービス装置 350 は、この認証が有効である場合、サービスをユーザに提供する。この場合も、第 3 の実施例と同様に、ユーザ識別コード格納部 133 の代わりにユーザ情報格納部 131 とすることもできる。

【0044】このような構成を用いることで、指紋認証カードの情報を暗号化し、安全に通信路を用いて伝送可能であり、サービス提供者は認識装置やサービス装置をカードリーダーと離れた場所に設置することが可能となり、認識装置、指紋データベース 700 やサービス装置 350 の集約等が可能となる。

〔第 5 の実施例〕本実施例は、カードリーダー 200 の出力、つまり、ユーザの指紋情報を蓄積する例を説明する。

【0045】図 9 は、本発明の第 5 の実施例の認証システムの構成を示す。同図に示す指紋認証カード 100 は、前述の第 3 及び第 4 の実施例と同様に、認証機能はない。同図に示すシステムは、カードリーダー 200 に蓄積装置 1000 が接続され、当該蓄積装置 1000 にはユーザの利用履歴を蓄積するための利用履歴データベース 1100 が接続されている。また、蓄積装置 1000 には、サービス装置 360 が接続され、サービス装置 360 からユーザに提供したサービスの利用情報が蓄積装置 1000 に送付される。

【0046】ユーザは、指紋認証カードをカードリーダー 200 に挿入し、指紋センサ装置 110 に指を乗せる。指紋センサ装置 110 で読み取られた指紋は、ユーザ識別コード格納部 133 に記録されたユーザ識別コードと共にカードリーダー 200 を介して蓄積装置 1000 に送信される。蓄積装置 1000 は、受信した指紋情報及びユーザ情報を、別途サービス装置 360 から送付されたサービスの利用情報と共に、利用履歴データベース 1100 に保存する。利用履歴データベース 1100 に格納されるレコードの例を図 10 に示す。

【0047】この手法では、指紋の認証を行わずに、指紋認証カードの利用者の指紋を利用履歴データベース 1100 に蓄積する。これを用いることで、クレジットカード利用時のサインと同様に、カード利用時の利用の証拠として指紋情報を残すことが可能となる。なお、本実施例においても、指紋認証カード内のユーザ識別コード格納部 133 の代わりに、ユーザ情報を記録した、ユーザ情報格納部 131 を用いてもよい。この場合、ユーザ識別コードの代わりにユーザ情報が転送される。

【0048】〔第 6 の実施例〕本実施例は、上記の第 5 の実施例の構成にカードリーダー 200 の出力を暗号化して蓄積装置 1000 に送る例を説明する。図 11 は、本発明の第 6 の実施例の認証システムの構成を示す。同図において、図 9 と同一構成部分には、同一符号を付し、

その説明を省略する。

【0049】同図に示す構成は、カードリーダ200で読み取られた指紋情報を暗号化装置800に転送する。暗号化装置800はカードリーダ200から取得した指紋情報及びユーザ情報を暗号化し、通信路を介して暗号復号装置900に送信する。暗号復号装置900は、信号を受信すると暗号化された指紋情報及びユーザ情報を復号化し、蓄積装置1000に出力する。蓄積装置1000は、復号化された指紋情報及びユーザ情報を別途蓄積したサービス利用情報と共に、利用履歴データベース1100に蓄積する。

【0050】上記の第5の実施例と同様に、ユーザが指紋認証カード100の指紋センサ装置110に指を載せると、当該指紋センサ装置110は、指紋を読み取る。読み取られた指紋情報は、ユーザ識別コード格納部133に記録されたユーザ識別コードと共に、暗号化装置800に転送される。暗号化装置800は、通信路を介して暗号復号装置900に渡すことにより、当該暗号復号装置900で復号化された指紋情報及びユーザ識別コードが蓄積装置1000を介して、利用履歴データベース1100に蓄積される。なお、この場合も、第5の実施例と同様に、ユーザ識別コード格納部133の代わりにユーザ情報格納部131とすることもできる。

【0051】このように、本実施例の構成は、ユーザの指紋情報を暗号化し、安全に通信路を用いて伝送可能であり、サービス提供者は蓄積装置1000や利用履歴データベース1100をカードリーダ200と離れた場所に設置することが可能となり、蓄積装置1000、利用履歴データベース1100等の集約等が可能となる。

【第7の実施例】本実施例は、指紋認証機能と指紋データメモリを従来のメモリカードに搭載した例を説明する。

【0052】図12は、本発明の第7の実施例の認証システムの構成を示す。同図に示すシステムは、指紋認証カードを用いずに、携帯型コンピュータ等に利用する、既存のメモリカードを用いる。メモリカード内に上記の実施例に示された指紋認証機能を付与する。以下では指紋認証カード100に代わるカードとしてメモリカード100の構成を説明する。

【0053】メモリカード100上に、指紋センサ装置110、認識装置120、指紋メモリ140、メモリ170及びメモリデータ送受信装置180を設ける。ユーザは、メモリカード100をスロット250に挿入し、このメモリカード100のデータへのアクセスが必要である場合に、指紋センサ装置110に指を乗せる。指紋センサ装置110は、指紋を読み取り、読み取られた指紋情報は、認識装置120に転送される。これにより、認識装置120は、指紋メモリ140に記録されている指紋と指紋センサ装置110で読み取られた指紋情報との照合を行う。照合が有効である場合のみ、メモリデー

タ送受信装置180が動作して、メモリ170と処理装置300との間でデータの送受が可能となる。

【0054】このメモリカード100は、指紋が認証されたときのみインターフェース回路であるメモリデータ送受信装置180が有効となり、処理装置300はメモリ170に対してアクセスが可能となるため、カードの所有者以外の人は読み書きができない。このため、秘密性の高いデータ等を格納しておくカードとして有効である。

10 【0055】本手法は、携帯型コンピュータ等の紛失し易い機器への応用が可能であり、万一機器を紛失した場合でもメモリに記録されているデータの流出を防ぐことが可能となる。

【第8の実施例】本実施例では、指紋認証装置と指紋メモリを既存の携帯機器に搭載した例を説明する。

【0056】図13は、本発明の第8の実施例の認証システムの構成を示す。同図に示す認証システムは、携帯機器1200上に前述の実施例の機能を搭載した構成である。携帯機器1200には、指紋センサ装置1210、認識装置1230、指紋メモリ1240、電源1250、電源回路1260、処理装置1270が搭載されている。

20 【0057】指紋センサ装置1210で読み取られた指紋情報が指紋メモリ1240に記録された指紋データと認識装置1230において照合される。電源回路1260は、認識情報の照合結果が有効である場合のみ、携帯機器の処理装置1270へ電源供給を開始する。このような携帯機器1200は、指紋が認証されたときのみ電源回路1260が動作し、処理装置1270が起動されるため、この携帯機器の所有者以外の者は利用できない。このため、当該携帯機器1200をユーザ以外の人に不正に使用されることを防ぐことが可能である。

【0058】本実施例における携帯機器の例として、特に携帯型コンピュータや携帯電話等の紛失し易い機器が挙げられるが、それ以外の据え付け機器のユーザ以外の人

30 【0059】

【発明の効果】上述のように、本発明によれば、あるサービスを受けようとするユーザに、当該ユーザ本人である場合にのみサービスを提供する装置に対し、ユーザが指紋認証装置を埋め込んだカードを用いて、従来、暗証番号やパスワード等で行っていたユーザの認証を指紋情報を用いて行い、サービスを安全に提供することが可能となる。これにより、ユーザやサービス装置の作業を簡略化できると共に、暗証番号やパスワードの盗難等による被害からユーザ及びサービス提供者を守ることができる。

50 【図面の簡単な説明】

【図 1】本発明の認証システムの構成図である。

【図 2】本発明の指紋認証カードに搭載される指紋センサ装置の例である。

【図 3】本発明の第 1 の実施例の認証システムの構成図である。

【図 4】本発明の第 2 の実施例の認証システムの構成図である。

【図 5】本発明の第 2 の実施例のユーザ情報データベースに格納されるレコードの例である。

【図 6】本発明の第 3 の実施例の認証システムの構成図である。

【図 7】本発明の第 3 の実施例の指紋データベースの例である。

【図 8】本発明の第 4 の実施例の認証システムの構成図である。

【図 9】本発明の第 5 の実施例の認証システムの構成図である。

【図 10】本発明の第 5 の実施例の履歴データベースの格納されるレコードの例である。

【図 11】本発明の第 6 の実施例の認証システムの構成図である。

【図 12】本発明の第 7 の実施例の認証システムの構成図である。

【図 13】本発明の第 8 の実施例の認証システムの構成図である。

【図 14】従来の第 1 の認証システムを説明するための図である。

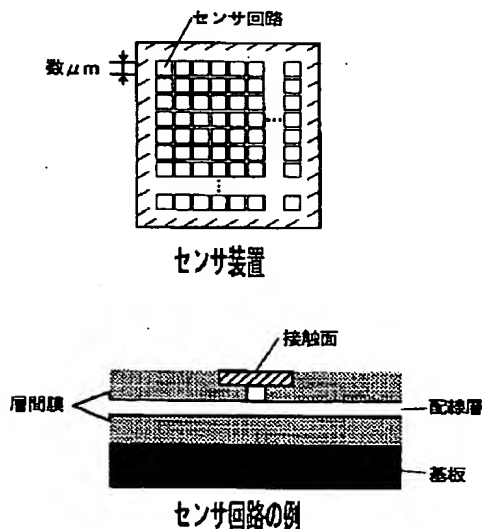
【図 15】従来の第 2 の認証システムを説明するための図である。

【符号の説明】

- 100 指紋認証カード
- 110 指紋センサ装置
- 120 認識装置
- 130 データチップ
- 133 ユーザ識別コード格納部
- 140 指紋メモリ
- 150 インタフェース部
- 170 メモリ
- 180 メモリデータ送受信装置
- 200 カードリーダー
- 300 処理装置
- 350, 360 サービス装置
- 400 検索装置
- 500 ユーザ情報データベース
- 600 認証装置
- 700 指紋データベース
- 800 暗号化装置
- 900 暗号復号装置
- 1000 蓄積装置
- 1100 利用履歴データベース
- 1200 携帯機器
- 1210 指紋センサ装置
- 1230 認識装置
- 1240 指紋メモリ
- 1250 電源
- 1260 電源回路
- 1270 処理装置

【図 2】

本発明の指紋認証カードに搭載される指紋センサ装置の例



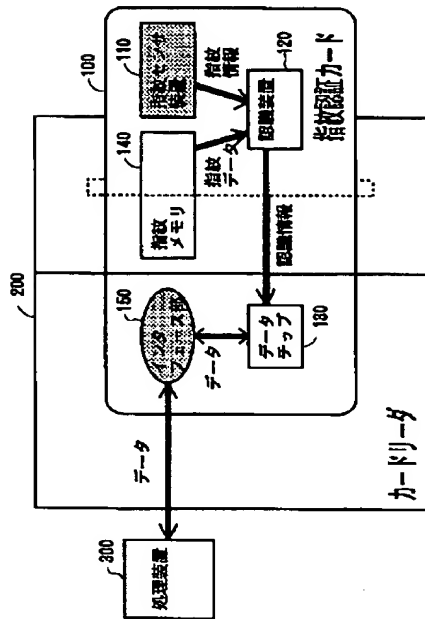
【図 5】

本発明の第 2 の実施例の
ユーザ情報データベースに格納されるレコードの例

ユーザ識別コード	ABC01234
ユーザ情報	
氏名	○山 ×夫
住所	○○県××市△△丁目
年齢・性別	男・□□才
利用可能サービス	○×銀行キャッシュサービス △□バス
⋮	⋮

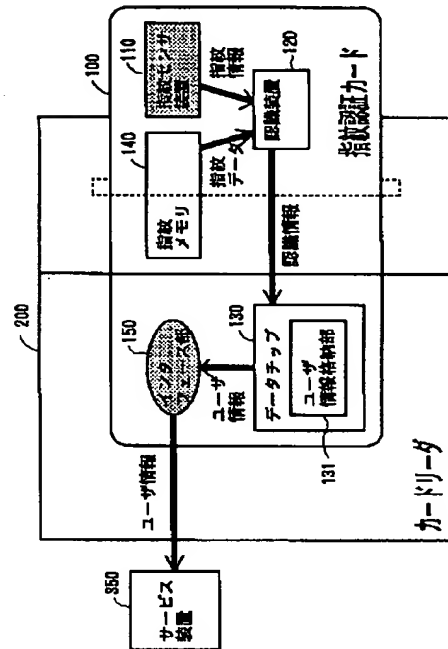
【図 1】

本発明の認証システムの構成図



【図 3】


本発明の第 1 の実施例の認証システムの構成図



【図 7】


本発明の第 3 の実施例の指紋データベースの例

700

ユーザ識別コード	ABC01234
ユーザ情報	
氏名	〇山 ×夫
住所	〇〇県××市△△丁目
年齢・性別	男・□□才
利用可能サービス	〇×銀行キャッシュサービス △□バス
...	...
認証用指紋情報	

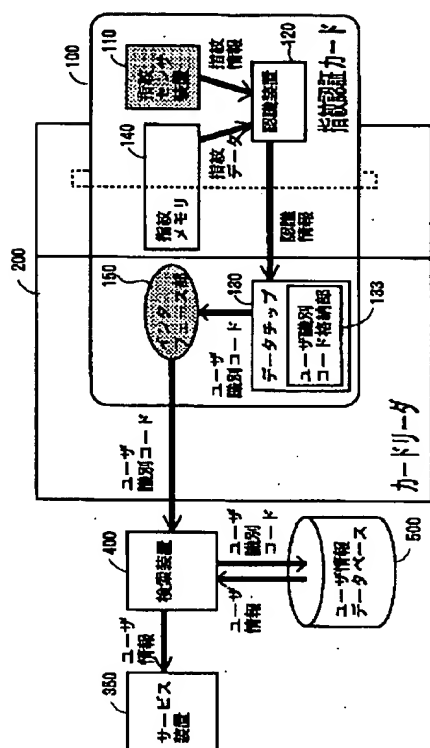
【図 10】

本発明の第 5 の実施例の
利用履歴データベースに格納されるレコードの例

ユーザ識別コード	ABC01234
利用情報	
利用時刻	〇〇年×月×日△時△分△秒
利用サービス	電子決済
利用施設	〇〇レストラン
利用内容	ランチA 1,200 ランチB 1,500
...	...
利用確認指紋	

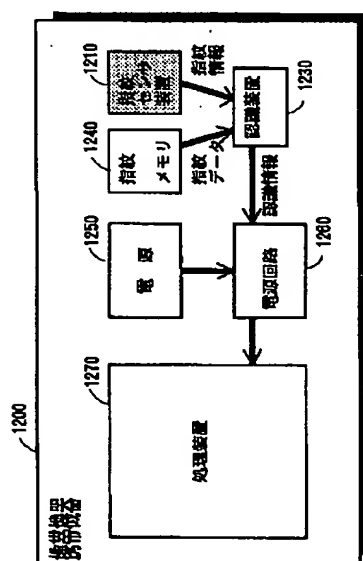
【图 6】

本発明の第３の実施例の認証システムの構成図



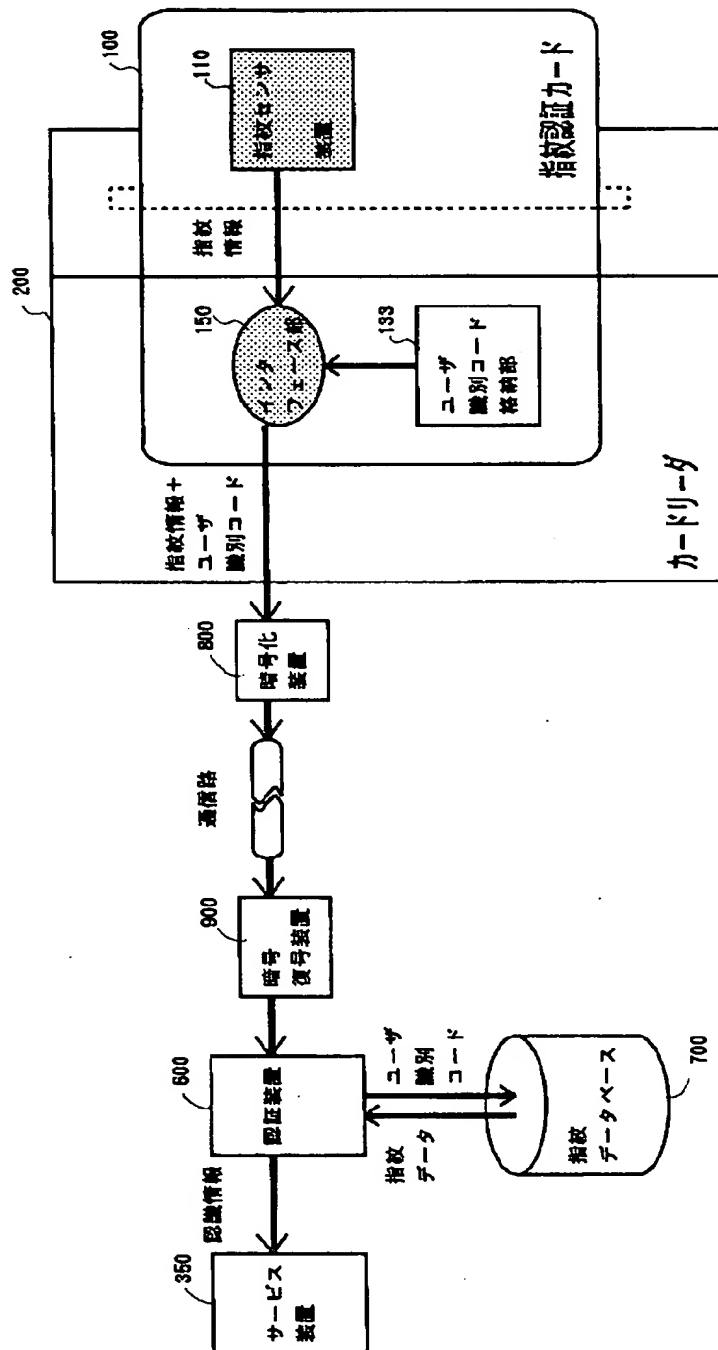
【図 13】

本発明の第 8 実施例の認証システムの構成図



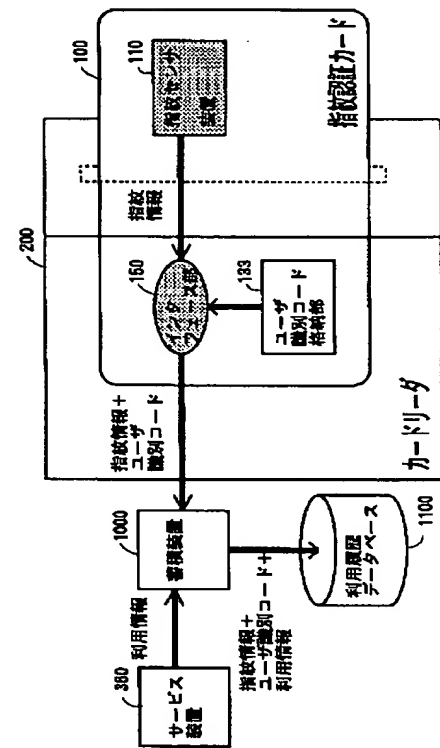
【図 8】

本発明の第 4 の実施例の認証システムの構成図



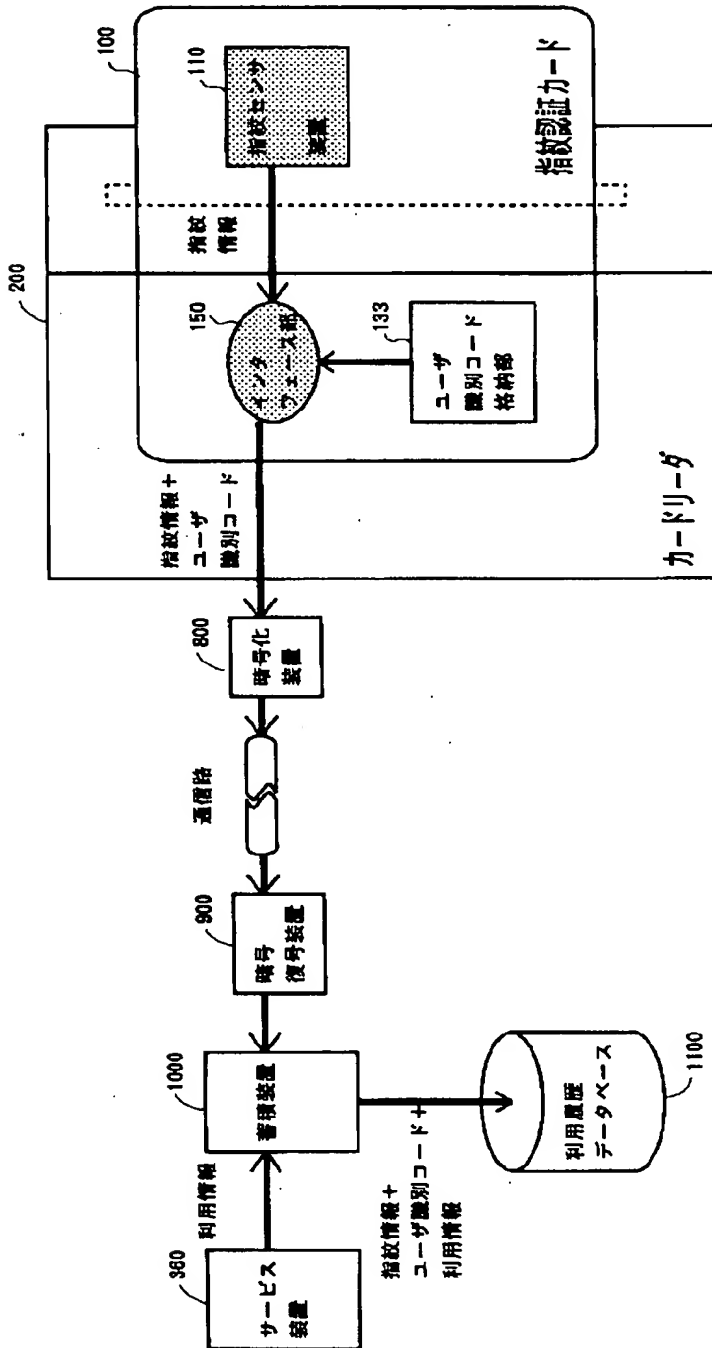
【図 9】

本発明の第 5 の実施例の認証システムの構成図



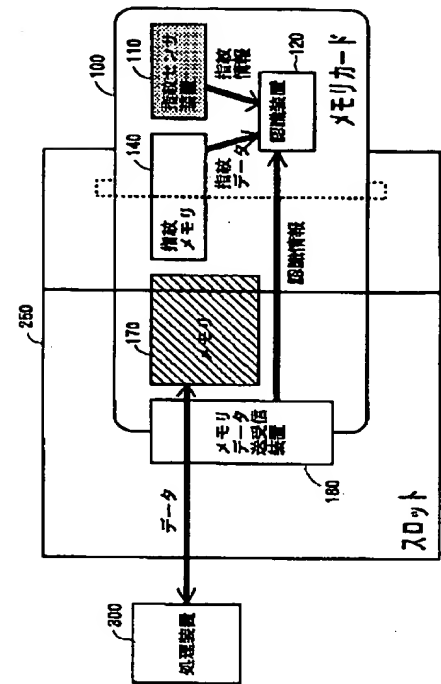
【図 11】

本発明の第 6 の実施例の認証システムの構成図



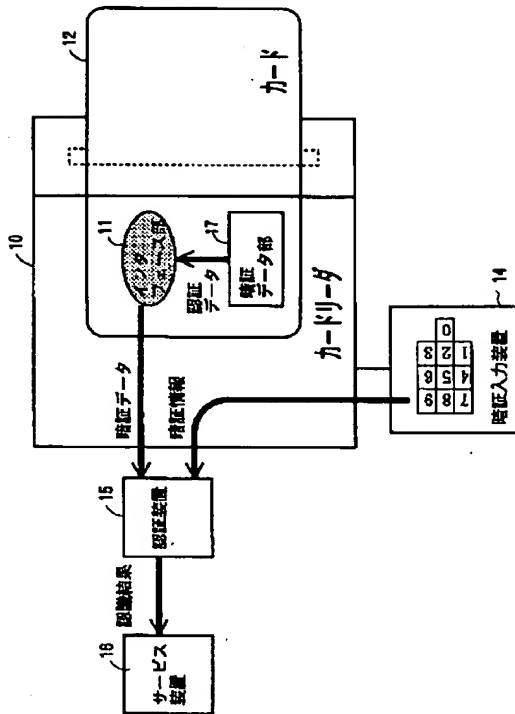
【図 12】

本発明の第 7 の実施例の認証システムの構成図



【図 14】

従来の第 1 の認証システムを説明するための図



【図 15】

従来の第 2 の認証システムを説明するための図

